AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Samuel Morgan, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I make this affidavit in support of an application for a criminal complaint and arrest warrant charging Alec Tahir Baker (Baker), year of birth 1964, with Wire Fraud, in violation of 18 U.S.C. § 1343, Bank Fraud, in violation of 18 U.S.C. § 1344, Conspiracy to Commit Wire and Bank Fraud, in violation of 18 U.S.C. § 1349, Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h), Operating an Unlicensed Money Transfer Business, in violation of 18 U.S.C. § 1960, and Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A.

2. The facts set forth in the Affidavit are based on my personal observations, my training and experience, information obtained from other agents, witnesses, and records obtained during the course of the investigation. Because I submit this Affidavit for the limited purpose of showing probable cause, I have not included in this Affidavit each and every fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue an arrest warrant for the individuals identified herein and to seize the bank accounts set forth herein. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. AFFIANT BACKGROUND

3. I am a Special Agent of the Federal Bureau of Investigation (FBI) in Providence, Rhode Island, duly appointed according to law and acting as such. I have been employed with the Federal Bureau of Investigation (FBI) as a Special Agent since 2018. From July 2018 to October 2020, I was assigned to work counterintelligence matters in the FBI Washington Field

Office. From October 2020 to January 2023, I was assigned to the FBI San Juan Field Office where I worked investigations involving complex financial crimes, including matters involving fraud and theft of cryptocurrency. From January 2023 to present I have been assigned to an FBI Cyber Task Force, in the San Juan Field Office from January 2023-February 2024, and in the Providence Office from February 2024- present. I have conducted numerous complex investigations concerning computer crimes and fraud, including wire and mail frauds, intrusions (i.e., gaining access to a protected computer or computer network without permission), and the use of botnets (i.e., a group of computers controlled without the knowledge of the computers' owners). I have experience reviewing records related to computer crime and fraud, including Internet Protocol ("IP") address logs used by computers on the Internet, network access logs, and security programs. I also have experience debriefing defendants, witnesses, informants, and other persons involved in computer crime and fraud. I have personally conducted and have been involved in numerous investigations that included the execution of search warrants involving electronic evidence and have been involved in all phases of investigations of computer intrusions.

4. In my training and experience, I know that fraudsters and individuals who conduct Business Email Compromise ("BEC") and other schemes often work with a vast network of money launderers to help them "clean" funds and then re-integrate the "cleaned" funds into the economy so that the funds can be used free from the taint of criminal activity. This allows the scammers to profit from their fraudulent conduct and to avoid getting caught. To these ends, scammers work with suspected money launderers to use, and recruit others to use, multiple bank accounts to move money in a series of convoluted transactions that makes it harder to identify the source of or who controls the funds. This is often referred to as "layering" or

"funneling." The use of "money movement" bank accounts ("movement accounts") to layer or funnel fraud often works as follows:

a. A few days before or around the same time that the fraud scheme is being perpetrated, a money mover is recruited to open a movement account(s). Sometimes, a movement account may be opened 60-120 days prior to execution of a fraud scheme so as to allow a "cooling off period" (banks more carefully scrutinize transactions made to newly opened accounts, and sometimes banks place limitations on how soon after opening an account funds deposited to the account can be withdrawn).

b. The movement account(s) receive fraud proceeds.

c. Within several days to weeks, and following the direction of a person connected to the fraud, a money mover will engage in transactions with the funds in various ways—for example, by withdrawing large amounts of cash from the movement account (sometimes obtaining cashier's checks with those funds), or using checks, ACH/wire transfers, or debit cards to withdraw cash in order to redistribute the fraud proceeds to others. The funds are sometimes converted to and/or moved via cryptocurrency.

d. Often, the beneficiaries of the transactions are other movement accounts; these movement accounts in turn use the funds they receive to conduct additional financial transactions with the funds. The purpose of these transactions is to further obfuscate the connection between the source of the funds and the perpetrators of the schemes.

e. After the funds are depleted, a money mover will often close the movement account(s). Sometimes, banks will freeze or close accounts they come to suspect are being used to launder funds from fraud or other criminal activity.

III. PROBABLE CAUSE

Overview of Baker's Criminal Conduct

5. As described in detail below, investigation to date has revealed that defendant Alec Baker is a key participant in a multimillion-dollar fraud and money laundering conspiracy. In this conspiracy, victims around the country are subjected to business email compromises in which their computer networks are compromised and funds are transferred to Baker's account and accounts of co-conspirators without the knowledge or consent of the account owners. Baker's role in this conspiracy is to receive the millions of dollars of fraudulent proceeds into one of dozens of bank accounts he established and to forward large portions of those fraud proceeds to others. Investigators have to date identified 7 different victims of this scheme, discussed below, who have collectively lost approximately $8,854,243. Of this total loss, Baker received at least $7,649,876 million in fraudulent proceeds into at least 6 of the 43 different bank accounts he opened in his name and in the names of various shell companies he established. After receipt of fraudulent proceeds, Baker conducts a wide range of transfers to additional financial accounts under his control, including dozens of additional bank accounts under Baker's control, the purchase and subsequent transfer of cryptocurrency funds, and transfers to other individuals with unknown relationships to Baker. Investigation has also revealed that Baker has full knowledge that the funds he is moving through his accounts were fraudulently obtained and that he is engaged in money laundering in return for a "cut" of the money he launders.

Town of [redacted], Rhode Island E-Mail Compromise

6. In January 2023, the FBI opened an investigation into an apparent business email compromise (BEC) in which the Town of [redacted], Rhode Island was defrauded of hundreds of thousands of dollars. Further investigation identified Alec Tahir Baker as the owner of a financial account that received funds from the BEC incident.

7. On January 20, 2023, the [redacted], Rhode Island (RI) Police responded to [redacted] Town Hall to take a fraud report from the town treasurer, S.H. S.H. reported that she was notified by the Deputy Treasurer, C.C., about two large withdrawals observed on the town general revenue account associated with Citizens Bank. S.H. stated that upon observing the two withdrawals, it was apparent that it was fraud as neither withdrawal was authorized. The two unauthorized withdrawals were observed to be on 01/19/2023:

a. $310,500 to United For Energy & Co Bank Code 208084707 entered on 01/19/23 at 03:13 pm and approved on 01/19/23 03:19 pm.

b. $210,500 to Al Hujen Group Oil Bank Code 32227124 entered on 01/19/23 at 03:23 pm and approved on 01/19/23 03:24 pm.

8. S.H. reported that the funds were sent via an ACH payment. ACH, known as an automated clearing house, is a computer-based electronic network for processing transactions such as the two above unauthorized transactions.

9. C.C. later reported to the [redacted] PD additional fraudulent payments of $86,345.21 and $123,618.65 were conducted on the town's account in the same scheme.

10. S.H. reported that the Town of [redacted] used the company FreedomTech for all its IT needs. S.H. reported that FreedomTech was contacted and advised they would check the system for any breach and or cyber-attacks. S.H. also reported that access to the Citizens Bank

account is only done via the hard drive computer and never through an application on a phone or any other device.

11. On January 23, 2023, S.H. reported to the [redacted] Police that she spoke with [redacted]'s Municipal Operations Manager and the Municipal Operations Manager told S.H. that someone visited the town's website before the transfers occurred and accessed the information for the previous town treasurer.

12. On January 24, 2023, an investigator with Citizens Bank reported to the [redacted] Police that it appeared that the account was compromised internally, most likely with a phishing email with a link that would give someone access to the bank account.

13. On January 25, 2023, S.H. reported that on January 18, 2023, she opened an email which caused her email account to shut down. She was required to log back in to access her emails.

14. On January 25, 2023, FreedomTech reported the following:

> "From the information gathered it would seem the client inadvertently clicked on a bad link within an email which redirected to an email account login popup. After the credentials were input, they may have been used by the threat actors to masquerade as out client."

CitiBank Records

15. On January 19, 2023, $310,500 was sent from the Town of [redacted] Citizens Bank account to a bank account at CitiBank ending in X4707 under the name "United For Energy & Co."

16. A review of open-source documents revealed that United For Energy & Co. is registered with the Washington State Secretary of State with address 2756 Peachwood Cir

Corona, CA. Baker is listed as the Governor of the company and R.T. is listed as the registered agent. R.T.'s provided email account was alecbaker1964@yahoo.com and phone number was 949-998-0241. T-Mobile subscriber information for phone 949-998-0241 identified Alec Baker as the subscriber starting in September 2021.

17. A review of bank account X4707 showed a $310,500 wire transfer credit from [redacted] Corp Pay on January 19, 2023. On January 20, 2023, there is a $75,000 debit with the note Q1 salary. On January 23, 2023, there is a withdrawal for $144,700. On January 31, 2023, there is a withdrawal for $2,264.

18. The January 23, 2023, withdrawal was used to purchase a bank check from United For Energy & Co to a company named D Light Agency LLC that was deposited into a JP Morgan Chase account.

19. CitiBank was able to provide photographs from their security cameras for the January 23, 2023, and the January 31, 2023, withdrawals. The photographs depict a male who appears to match Baker's California DMV photo.

20. Based on my training and experience, these transactions are consistent with the laundering of fraud proceeds. The fraud proceeds are deposited into an account and are moved out shortly after.

Baltimore County Police Investigation

21. Approximately eight months before the [redacted], Rhode Island compromise described above, on May 22, 2022, the Baltimore County Police Department were dispatched to [redacted] in Glencoe, MD for a report of theft/fraud by wire. The responding officer met an individual named E.M.

22. E.M. reported that she manages the finances for [redacted]. E.M reported that on May 13, 2022, she logged into the company's bank account and noticed two wire transfers that were not authorized. E.M. reported that she called the company's bank, and the bank informed her that someone called the bank and said they were E.M. and asked that an activation code be emailed to them. The bank sent an email to the email address they had on record for E.M.

23. The bank reported that because the unknown person had the activation code, they could initiate wire transfers from the [redacted]. bank account.

24. Investigators later determined that E.M.'s email account had been compromised. They determined that a rule had been set up on E.M.'s email that would send emails sent to her account to the archives folder and not notify her that an email had been received.

25. One of the wire transfers was for $120,000 to United for Energy and Consulting at a Bank of America account with account holder Alec T. Baker.

26. Bank of America provided photographs of withdrawals being conducted off this bank account shortly after the $120,000 was transferred in and they appeared to match the California driver's license photograph of Alec Baker.

27. On August 31, 2022, the Baltimore County Police spoke to Alec Baker along with Baker's attorney. Baker reported that he was the victim of an online romance scam. Baker told investigators that he reported this incident to the Corona, California Police Department.

28. According to Corona Police Records, on August 30, 2022, Baker called the Corona Police to report that someone was using his information to try to open accounts, taking money out of his account and sending him mail. Baker utilized phone number 949-998-0241 to call the Corona Police.

29. Baker's story to the Corona Police does not appear to coincide with the fact that Bank of America provided photographs of Baker withdrawing the money to the Baltimore County Police.

30. Baker provided a series of WhatsApp messages to the Baltimore County Police that he was having with someone named "Investor 2." The first message that Baker provided to the police stated, "I have a conference call tomorrow with the police 8 am you think they will leave me alone." The rest of the messages that Baker provided appeared to come after that first message.

31. Baker did not provide any documentation to the Baltimore County Police that predated the message regarding meeting the police.

32. Based on my training and experience investigating romance scams, the victims usually have a large quantity of messages between themselves and the scammer that span months and years. It is out of the ordinary that Baker only had a single day of messages to provide to law enforcement. I also believe that Baker was attempting to minimize his involvement in the laundering of the fraud proceeds. He told the Corona Police that someone was moving money out of his account when Bank of America provided photographs of Baker himself withdrawing the money.

33. The Baltimore County Police sent a money mule warning letter on Baker via certified mail. The receipt of the mail on September 10, 2022, appeared to be signed by Alec Baker. The letter read:

> " The Baltimore County Police Department, Financial and Cyber Crimes Team, is providing warning that you, and/or persons you associate with, may be engaged in fraudulent activity that violates state and/or federal criminal laws. Your recent

transmission and/or receipt of money via wire transfer may have facilitated the transfer of money from the victims of a crime, to the perpetrators of a fraudulent scheme.

Specifically, a $120,000.00 wire you received on or about May 13th, 2022 was determined to be a part of a fraud scheme, and was stolen from a business operating in Baltimore County.

Some fraudulent schemes involve criminals who falsely represent themselves as someone else, in order to trick victims into sending money via wire transfer to an identified pre-determined account (e.g. your bank account). The criminal may ask the account holders, such as yourself, to "process payments", "transfer funds", or "re-ship products" to facilitate the movement of money obtained through fraud from victims to the criminals. These requests may be masqueraded as work from home, secret shopper opportunities, or an online romance. Under certain circumstances, knowingly engaging in a financial transaction that involves funds derived from illegal activity may violate the federal money laundering laws, even if you had no involvement in the underlying criminal activity. Under certain circumstances, you may also have a legal obligation to inquire about the source of the funds and may not avoid legal responsibility by being willfully blind to the source of funds. A knowing and intentional violation of the money laundering laws may result in criminal prosecution and the seizure of property that is found to be tainted by illegal funds. By agreeing to engage in such transactions, you may also be facilitating a fraudulent scheme and assisting the perpetrators of the scheme."

Bank of America and Coinbase Records

34. Records provided by Bank of America identified the receipt of funds by Baker utilizing Bank of America account x9740 under the company name United for Energy Consulting on May 13, 2022. On May 18, 2022, $117,800 was transferred by Baker to another Bank of America account maintained by Baker under his name, account x3425. From account 3425, $110,700 ultimately went to a Coinbase account under Baker's name. Coinbase records for Baker identified an account under his name created on April 11, 2022. From April to September 2022, Baker deposited over $787,000 into this Coinbase account, ultimately purchasing over $772,000 worth of Bitcoin and other cryptocurrencies, which he then sent on to different cryptocurrency addresses. Additionally, Coinbase records indicate Baker used an iPhone to login to his account on multiple occasions. Based on my training and experience, Baker's activity receiving fraudulently obtained funds, converting them to cryptocurrency and subsequently sending the cryptocurrency to an actor overseas is money laundering activity and conducted to evade law enforcement.

[redacted] *Business Email Compromise*

35. On July 13, 2022, the Hartland, Wisconsin Police were dispatched to [redacted]. Once on scene, they met with an individual named A.W. who reported that she was an accounting supervisor at [redacted].

36. A.W. reported that she had received an email on May 22, 2022, from a vendor named Nano Solutions asking A.W. to change their bank payment information. A.W. changed the bank information.

37. A.W. realized that the email was fraudulent when she looked back and realized that there was a letter missing from the email addresses the request came from. By the time it

was identified as being fraudulent, [redacted] had already sent 5 payments totaling $325,496.02.

38. The Hartland Police determined that the payments were sent to a Bank of America account and served legal process to determine the account holder and get other banking information.

39. Bank of America reported that the account was held by "United For Energy & Consulting Inc." with Alec Baker as the signer. The account information obtained by the Hartland Police matched the Bank of America records obtained by FBI legal process above for account 9740. Hartland police also received returns for Bank of America account 3425 outlined above.

40. The Hartland Police reviewed the bank statements for May and June 2022 and noted that there were large wire transfers in followed by wire transfers out for the same amount. The Hartland Police also noted that there were ATM withdrawals in Corona, California, a location Baker's family lives in and a Zelle transfer to H.H., who is known to be Baker's wife.

41. Based on my training and experience, Baker making large wire transfers out for the same amount is consistent with money laundering activities. Based on the withdrawals in Corona, CA where Baker is known to sometimes reside, as well as transfers to his wife, I do not believe Baker's information is being used by someone other than himself. Furthermore, I believe Baker is the one conducting the money laundering transactions.

Blue Ribbon Builders

42. On November 7, 2023, victim P.Z., along with his financial advisor, came to the Genesee County Sheriff's Office ("GCSO") in Batavia, New York to report a larceny of stolen money though fraudulent financial transfers.

43. P.Z. stated that he is building a home in Montana using a company named Blue Ribbon Builders. As part of the building process, P.Z. sent installments of payments for services rendered. P.Z reported that recently he received an email, which he could no longer locate, requesting that payments be directed to a different bank account at American First Credit Union with account number ending in x8215.

44. P.Z. reported that on November 3rd or 4th, 2023, he received an email from someone at Blue Ribbon Builders advising that they had not received the 5th and 6th payment installments. P.Z checked and reported that the payments had been made.

45. P.Z. investigated the issue along with some IT personnel and discovered that the recent emails had come from blueribonbuilders.com which is missing a "b" in ribbon. This was different than the actual email address that had 2 b's in ribbon.

46. P.Z. reported that the 5th payment installment was for $400,000 and the 6th payment installment was for $137,854.95.

47. GCSO sent a subpoena for bank records for the account at American First Credit Union. The bank reported that the account belonged to Baker Global Services LLC. The person responsible for the account was listed as Alec Baker, with DOB ending in 1964. Bank documents showed that Baker listed his address at 7407 Dragonfruit Ave Las Vegas, NV, his phone number as (949) 998-0241 and his email address as alecbaker1964@yahoo.com.

48. A review of the American First Credit Union bank account records showed an account balance of $6,900.65 on October 10, 2023. On October 10, 2023, there is a deposit for $400,000 from P.Z.

49. On October 11, 2023, the deposit posted to the account. On this same date, $6,900 was transferred to a shared savings account, leaving the account balance at $400,000.65. Based

on my training and experience, I believe Baker did this to keep his own money separate from the incoming fraud proceeds in the event the bank put a hold on his account for receiving the fraudulent money.

50. On October 13, 2023, bank records show a second deposit from P.Z. for $137,854.95.

51. Between October 10, 2023, and October 20, 2023, Baker conducted multiple bank to bank transactions totaling $527,136.22, leaving the account with a balance of $10,719.38. These transfers included a total of $63,080 transferred to an individual named F.N., $199,216 transferred to an individual named T.P., $191,360 transferred to an individual named S.T., and $74,000 transferred to a personal account in the name of Baker, among other transactions.

52. Based on my training and experience, these transactions are consistent with the laundering of fraud proceeds.

53. Detectives from the GCSO conducted a search warrant of Baker's email address, alecbaker1964@yahoo.com, and provided the results to the FBI. The results included Baker's communications to and from multiple financial institutions.

[redacted] *Business Email Compromise Incident*

54. On December 18, 2023, J.A. who is a third-party attorney for [redacted], reported to the FBI that [redacted] was the victim of a BEC scheme. [redacted] is an American Defense Contractor based in Colorado.

55. J.A. reported the following: Between April 2023 and September 2023, [redacted] made 21 ACH payments to subcontractor Quantum Dynamics, Inc. ("QDI")—totaling $4,525,978.56—which were apparently redirected to a fraudulent entity. These payments were made under the instructions of A.W., a contracts administrator at QDI, by her regular email

address. [redacted] bank, Citibank, made the 21 ACH payments to three banks: Bank of the West, Citibank, and Banner Bank.

56. Banner Bank provided documents and emails pertaining to the fraudulent transfers in response to a subpoena. The same emails were provided to the FBI from GCSO in relation to their investigation on the Blue Ribbon Builders email compromise in which Baker was identified. The emails from GCSO came from a Search Warrant conducted for alecbaker194@yahoo.com, the account used by Baker to exchange emails with Banner Bank. The following email exchanges were identified relevant to this scheme:

57. In one email exchange, T.W., a Banner Bank employee, asked Baker for clarification regarding large scale wire transfers from [redacted] with the notation "Quantum Dynamics" coming into Baker's account at Banner Bank.

58. Baker responded with the following from account alecbaker1964@yahoo.com on October 10, 2023:

> "Hello T.W.
>
> I hope this email finds you well. I wanted to provide some clarification regarding the payments coming in from [redacted] with the notation that they are for Quantum Dynamics. Quantum Dynamics is a trusted business partner with whom I have an ongoing professional relationship. We have been collaborating on various projects and ventures and as part of our financial arrangements [redacted] often processes payments on their behalf for services rendered. Thank you for your attention to this matter and I appreciate your understanding and cooperation in ensuring the smooth processing of these payments."

59. Also found in the subpoena returns from Banner Bank were two invoices provided by Baker from Al Hujen Group. These invoices were dated August 28, 2023. These invoices were for customer Vectrus. The invoices were for $550,545.59 and for $204,382.46.

60. Both invoices state they were for "Dell Servers" in the details section.

61. At the bottom of each invoice a bank account at Banner Bank for Al Hujen Oil and Gas lists Alec Baker as the CEO along with his known phone number and Yahoo email address. On January 26, 2024, the FBI interviewed J.A., the third-party counsel for [redacted]. J.A. reported that [redacted], their client, has never seen these invoices, that they do not appear to be real and that [redacted] has not purchased any servers recently.

62. Baker also provided Banner Bank with a contract between [redacted], Al Hujen Group for Oil and Gas, and QDI, supposedly signed by representatives from all three companies. FBI interviews conducted in August and September 2024 with Vectrus and QDI representation confirmed neither [redacted] nor QDI had a contract with Al Hujen or Baker. Based on the interviews from [redacted] and QDI representatives, I believe Baker created and sent fraudulent invoices to Banner Bank in order to obtain the release of fraudulently obtained funds.

63. Another email from Baker to Banner Bank stated the following:

> "Hello T,
>
> In reference to the required document backing up the purpose of payment to [T.P.]: Please find the attached invoice for purchase and services provided. I would like to state clearly that both Baker global and United for energy are my business account with other banks and the purpose of the funds sent there are business related.
>
> Regards,

Alec Baker

CEO

Al Hujen Group for Oil & Gas Services Inc

(949) 998-0241

64. Baker attached three invoices to the email. Two of the invoices were bills from "Propst Companies," utilizing the legitimate logo of Propst Companies, a commercial real estate company based in Huntsville, Alabama. T.P. was listed as a "Logistics Manager" in both invoices. R.D., an employee at Propst Companies, was contacted by the FBI and stated both invoices were fraudulent, and T.P. had never been employed by Propst Companies.

Interview of R.K.

65. In October 2024, FBI Agents interviewed R.K., a United States-based individual who has received approximately $2,370,158 in fraudulently obtained funds from Baker or Baker owned business accounts since August 2023. R.K. also maintained a Coinbase account in which he deposited over $1.4 million from December 2022 to August 2023. R.K. subsequently purchased multiple cryptocurrencies to include Bitcoin (BTC), Tether (USDT), and Ether (ETH). After purchasing cryptocurrency, R.K. sent the funds to other cryptocurrency addresses. R.K. told agents he conducted the activity on behalf of an individual he met via LinkedIn named "Olivia Myers." R.K. conversed with Myers via text, email, and WhatsApp. The individual provided a photo of her California Driver's License, but the license name and number do not match California DMV records. R.K. never met Myers in person. R.K. knew Baker's name, as well as the company "Baker Global Services." R.K. did not know who Alec Baker was, but was aware he received funds from him on multiple occasions. As recently as October 1, 2024, R.K. received $44,275.93 from Baker into a checking account maintained by R.K. R.K. was unaware

of the origin of those funds but Myers regularly contacted R.K. to send the funds to other individuals.

66. When R.K. began ignoring "Myers" after speaking with FBI Agents, Myers began aggressively messaging R.K. and threatening him regarding the $44,275.93 he was in possession of. Based on my training and experience, "Myers" is using stolen or fraudulent identities and using R.K. to launder funds received from Baker.

67. Myers told R.K. the funds he was receiving and sending were for Myer's fashion design business. R.K. never met Myers nor Baker in person and was unsure how Baker and Myers were in business together.

Ongoing Money Laundering by Baker in 2024

68. In January 2024, California based company [redacted] reported a BEC incident in which they sent $2,377,414.49 to an account they thought belonged to a vendor. $2,377,414.49 was transferred to Fifth Third Bank account x6213 under the company name Wall Edge Inc. Account documents for x6213 identified Baker as the only signor on the account. After receiving the $2,377,414.49, Baker sent funds to another financial account under the name Al Hujen Group with Baker as the signor, as well as eight additional recipients including R.K. and other companies.

69. In July 2024, Michigan-based company [redacted] was the victim of a BEC scheme. [redacted] sent $657,000 to an account they thought belonged to a vendor. The vendor sent an email changing the wire instructions to instead go to a Plains Capital Bank account belonging to Alec Baker. The $657,000 went to a financial account belonging to Alec Baker, who within days moved the funds to other accounts under his control and under the

control of others. Investigators are in the process of obtain the full banking records for these 2024 money laundering transactions involving Baker.

Financial Accounts Identified

70. Investigation identified the following accounts for Baker. Baker utilized at least 43 bank accounts at 13 different financial institutions and evidence to date indicates additional financial institutions where Baker opened or attempted to open an account.

Institution	Account #	Account Name
American First	8215	Baker Global Services
Banner Bank	6408	Al Hujen Group for Oil & Gas Services, Inc.
Banner Bank	6506	Alex Tahir Baker
BoA	1576	Al Hujen Group for Oil & Gas Services, Inc.
BoA	3336	Alec Baker
BoA	3425	Alec Baker
BoA	4475	Alec Baker
BoA	7073	Alec Baker
BoA	7758	Al Hujen Group for Oil & Gas Services, Inc.
BoA	7980	Alec Baker
BoA	9740	United for Energy & Consulting, Inc.
BoA	9766	United for Energy & Consulting, Inc.
California Bank	1336	Baker Global Services/ Alec Tahir Baker
California Bank	4665	Alec Tahir Baker
California Bank	0625	Wall Edge Inc.
California Bank	1252	Alec Tahir Baker
Citibank	4707	United for Energy & Consulting, Inc.
Citibank	0475	Al Hujen Group for Oil & Gas Services, Inc.
Comerica	8670	United for Energy & Consulting, Inc.
Comerica	9646	Alec Tahir Baker
Fifth Third	6213	Wall Edge Inc.
Fifth Third	7384	Alec Tahir Baker
Inwood	5211	Al Hujen Group for Oil & Gas Services, Inc.
Inwood	9219	Alex Tahir Baker
JPMC	3062	Alec Tahir Baker
JPMC	9180	United for Energy & Consulting, Inc.
Navy Fed	1584	United for Energy & Consulting, Inc.
Navy Fed	2329	Alec Tahir Baker
PNC Bank	1693	Alec Baker
PNC Bank	4847	United for Energy & Consulting, Inc.
PNC Bank	8407	United for Energy & Consulting, Inc.
PNC Bank	0574	Alec Baker
US Bank	1202	Alec Baker
US Bank	4259	Alec Tahir Baker
US Bank	6653	Al Hujen Group for Oil & Gas Services, Inc.
US Bank	7026	Alec Tahir Baker
US Bank	7209	Alec Tahir Baker
US Bank	8780	United for Energy & Consulting, Inc.
US Bank	0093	Al Hujen Group for Oil & Gas Services, Inc.
US Bank	0398	Al Hujen Group for Oil & Gas Services, Inc.
US Bank	0457	Alec Tahir Baker
Western Alliance/ Bank of Nevada	5756	Alec T Baker
Western Alliance/ Bank of Nevada	9972	Baker Global Services

Apple Search Warrant Returns

71. On September 19, 2024, a search warrant was served to Apple, Inc. for Baker's iCloud account, DSID's 20412265817 and 18566824009. Returns from Apple contained over 3,000 Voice Notes and over 42,000 images and videos. Review of the images identified multiple screenshots of bank accounts and cryptocurrency exchanges. Review of the voice notes identified hundreds of messages in which Baker appears to be sending voice messages via WhatsApp. The messages contained details about bank account opening and closing updates, questions and comments about specific amounts of funds that Baker received and was questioned about by banks, ideas by Baker to open new businesses and accounts in the United States, Kuwait and Iraq, discussion of Baker's "cut" and the "deal" Baker made with the recipient of the voice messages, and other updates on Baker's activities receiving, sending, and maintaining funds on behalf of the unidentified party.

72. To date, investigation has not identified the recipient of the voice messages or the specific date/time the voice notes were created or sent; however, the iCloud account where the voice notes were identified was created in September 2021, before the first known money laundering activity by Baker occurred in 2022. Summaries of some of the voice messages are included below with the file name of each voice message. The summaries are not verbatim. Baker's voice is audible in each voice message and Baker identifies himself in at least one message.

- **d0fa8573-2676-4eca-a876-9e3617bebfee.opus**: "No, no, no, I'm dealing with the biggest crook. *The only thing keeping us alive is there is honesty among crooks. I am becoming like you, one of the biggest crooks. No, no, no you're not no banker. You used to be a banker, now you are a big scam, just like I am."*

- **00e54292-2aab-418d-8d1a-3601f1853ad2.opus:** "*The bank called me, fraud fraud fraud. I'm becoming a fraud myself.* For heaven's sake, man, don't leave me like this open end, loose end. The 1.5 need to be covered immediately today. I'm talking about documents."
- **6fa621cf-cadf-45b0-a70c-e598cc156a20.opus:** "ok so the two banks are ready to go...you can absolutely use them."
- **04b0102f-ec97-40f4-aab6-641a2331e263.opus**: "In this case I have to rent an office in Washington...it's good to have an office there... I always like to have things real so justification because, you know, there is no way, you gotta have something to cover this bullshit. You know what I'm saying? Like cars. I'm thinking car lots immediately in Vegas."
- **0604419f-c45e-4e53-8415-2fec6330dd65.opus**: "Blocked blocked blocked. Still blocked. Can't do nothing....they could close you for any reason...until this moment it's on hold, blocked, I don't know what to do, just wait. I cannot argue more than that."
- **f391059c-840e-417e-a8d3-9438e684678d.opus:** *"I told you this from day one. If you leave money in the account it builds credibility with the bank. You guys don't wait. You always hurry. I don't know what's the rush for, they might lose or it or get caught, I know*. But moving money that fast brings a lot of attention. Especially with new accounts. I learn it the hard way...and that's why you ask me about old accounts at US Bank and Bank of America... again you need to establish credibility and time with these new banks, you can't just open accounts

and transfer 500 dollars to it... when you accept it and move it the next day it's a fraud alert, immediately."

- **82637718-4a84-4c94-a805-5d8b7919638b.opus**: "I know the work is here, but it has to be purchase equipment or cars and shipping. I mean, that's really a must because I don't want to face the same trouble as before. Has to be some kind of commodities vs whatever. *I guess in this case, it's like the old saying, this is just money laundering all the way down to hell.*"
- **9780b114-0ef0-451a-a2a8-86763148b5bc.opus**: "You keep reminding me of how much money we make, but you forgot the deal that we have. When we have a deal you do not come back and throw things in my face, please... I don't care about your people, I don't know them... *"*
- **92b2c0c3-e6a2-4d7b-ae28-5f9dc04d6aec.opus:** "*In case this thing goes very south, do you have a way of covering the money, in case, cause I know it's fraud, I know this money is bad, probably. Is there no way I can send the money overseas,* I can go overseas and send money there and cover it, just in case... if you can tell me how we can recover this amount, is this possible? I don't know what documents you can provide for these people and I'm sure you can't, so I don't know what's the solution.."
- **8819b2c-4325-42d3-bd02-408ce3fe27ee.opus:** *"It's a fraud dear. It's going to be headache again.* They're not going to leave it alone, they want their money back. Whoever, I don't know."
- **6e3e7a17-6530-4ccc-90f5-a857ebcea4a9.opus**: *"I wanted to get out of the country so we can establish something out of the country...rather than deal with*

*all these restrictions here... Kuwait I have open account since 2012...*I called them and you have to have your residency re-installed. I already have people waiting seem do the residency in no time..."

- **6db64901-2aea-4c2d-9f01-9a6f99d7d1b6.opus**: "*I told you. We need documents. If you can't provide documents, this is gone, we are history. They caught me for 90,000 and they make a hooplah. Now is 1.5 million and you think they're going to leave it alone?* And there's another check in Bank of America for $230,000. They're going to come up with shit that gonna put me down dear. *I'm fucked in this case if you don't help me out with documents and stuff. All the shit you are sending is fraud. It's not good. All of them are fraud.* Otherwise why they call? I told you these big numbers gonna give us bad news. You never listen."
- **2d25a65c-c194-49d0-9f6a-96cf84ad4d07.opus:** "And so I thought about it. I don't think we're going to be able to open any more accounts, that's for sure...banks are dropping. I don't know how many you want to keep... I think overseas is the ticket.... it's all up to you man...these transactions all gotta be...these transactions all repeat themselves... they become suspicious."
- **2752bc30-3d8b-4fd9-a91e-d83324d9338d.opus: "***And that's why we have a problem. Those banks, when they see the money comes in, large amounts, the next day they clear, and that's why we start having problems. The reason Bank of the West didn't have so many problems because I always leave some money in there. Same as Banner.* So when I do that, you need to help me out, like you always suggest. I don't want to have this discussion over and over."

73. Based on the above voice messages, Baker was plainly aware the funds he was receiving were fraudulent. Baker mentioned specific banks known to investigators in this scheme. Baker was proposing business ideas such as purchasing and reselling cars to launder the stolen funds, and was aware the banks were suspicious of his activities. Baker advised his unidentified co-conspirator about the issues with the manner they sent Baker funds and advised them on how to avoid detection. Baker is fully aware that he is involved in a scheme that he describes to be: "just money laundering all the way down to hell."

Conclusion

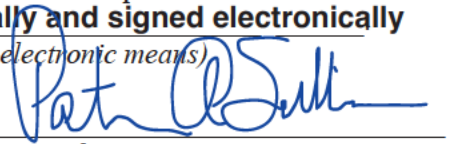
74. Based on the above activities conducted by Baker, including the opening of over 40 financial accounts, continued receipt and sending of fraudulently obtained funds over multiple years, providing of fraudulent invoices to banks to justify his receipt of fraudulent funds, discussion of his activities and acknowledgement of the fraudulent funds he received, and other activities outlined, I submit there is probable cause to believe that from in or about May 2022 through October 2024, defendant ALEC BAKER committed Wire Fraud, in violation of 18 U.S.C. § 1343, Bank Fraud, in violation of 18 U.S.C. § 1344, Conspiracy to Commit Wire and Bank Fraud, in violation of 18 U.S.C. § 1349, Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h), Operating an Unlicensed Money Transfer Business, in violation of 18 U.S.C. § 1960, and Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A.

I declare that the foregoing is true and correct.

Samuel Morgan
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Sworn telephonically and signed electronically**
(specify reliable electronic means)

November 1, 2024
Date



Judge's signature

Providence, Rhode Island
City and State

Patricia A. Sullivan, USMJ
Printed name and title